SEC103 - Droit, enjeux de sécurité, conformité

Valide le 25-04-2019

Code : SEC103

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Véronique LEGRAND

Contact national :
EPN 05 Informatique
2 rue conté
31.1.79
75003 Paris
01 40 27 20 38
Agathe Froger
agathe.froger@lecnam.net

Présentation

Prérequis

Bac+2 informatique, BAC + 2 SI ou SHS. Il est conseillé d'avoir suivi le module SEC001.

Objectifs pédagogiques

• Connaître les lois, règlements, politiques et éthique en matière de cybersécurité et de protection de la vie privée.

• Connaître les principes fondamentaux du droit appliqués aux nouvelles législations RGPD et LPM.

• Connaître les principes de cybersécurité et de confidentialité.

Compétences

Principes fondamentaux de droit, des lois du numérique et de sécurité numérique

RGPD, les différents volets sous l'angle du droit et de la technique

LPM, les différents volets sous l'angle du droit et de la technique

Outils et RGPD et LPM

Gouvernance nationale et internationale de la cybersécurité et de la sécurité des données

Programme

Contenu

Temps 1: principes

- Cours 1 : Principes fondamentaux de droit

o Sources du droit (directes et indirectes)

o Organisation juridictionnelle

§ Hiérarchie des normes

§ Présentation des lois, normes et standards,

national et international

o Domaine d'application de la règle de droit

o Preuves et sanctions

- Cours 2 : les lois du numérique et de sécurité numérique

o Principes fondamentaux de la république numérique

o Lois principales : LCN, Godfrain,

o Introduction aux lois LPM et RGPD

- Cours 3: Gouvernance nationale et internationale de la

cybersécurité et de la sécurité des données

o Gouvernance mondiale, européenne (organisme,...)

o Les organismes nationaux :

§ ANSSI et CNIL

Les organismes internationaux

- TD3 recherche et analyse d'un cas réel : présentation.

Temps 2 : RGPD, les différents volets sous l'angle du droit et de la technique :

- Cours 4 :

o Enjeux : propriétés (vie privée et traçabilité)

o Doctrine et stratégie de défense/attaque

o Cible, menace, vulnérabilités

- Cours 5 : (développé ensuite dans UE)

o Conformité du point de vue juridique

o Normes ISO 27x

o RGS

o PSSI et biens informationnels

o Objectifs, Mesures, indicateurs et tableau de bord spécifique)

- Cours 6 :

o Sanctions

o Organisation de la mise en place RGPD

§ Fonctions (DPO)

§ Responsabilités de l'entreprise

- TD6 RGPD

Temps 3 : LPM, les différents volets sous l'angle du droit et de la technique :

- Cours 7 :

o Enjeux : propriétés (DIC et traçabilité)

o Doctrine et stratégie de défense/attaque

o Cible, menace, vulnérabilités des IT

- Cours 8 : (développé ensuite dans UE)

o Normes ISO 27x

o RGS

o PSSI et IT

o Objectifs, Mesures, Indicateurs et Tableau de bord

- Cours 9 :

o Organisation de la mise en place LPM

§ SOC

§ Métiers

§ Outils

§ Responsabilités de l’entreprise

- TD9 LPM : mise en oeuvre au travers d’un cas d’étude suite de

TD6 RGPD

Temps 4 : Outils et RGPD et LPM

- Cours 10 : Découverte référentiels métiers

o TD10 : Exemples de référentiels pour les normes de sécurité

des données : Santé, PCI,…

- Cours 11 : Découverte big data

o TD11 : Big data : outils, méthodes et moteurs de recherche

dans le big data

- Cours 12 : Découverte IA

o Algorithmes : utilisation d’algorithmes de l’IA,

o TD12 : petit algorithme d’apprentissage

- Cours 13 : Découverte OC et cookies

- TD13 :

Modalités de validation

- Projet(s)
- Mémoire
- Examen final

Description des modalités de validation

Dossier cahier des charges d’analyse de risque ou d’une analyse

de sécurité ou de vulnérabilité

Ou examen sur table

Ou les 2